Multinational Experiment 7

"Access to the Global Commons"

OBJECTIVE 3.3 LEXICON AND ABBREVIATIONS

Version 1.1

28 May 2012

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
24 JUL 2013	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Multinational Experiment 7 "Access to the Global Commons" OBJECTIVE 3.3 LEXICON AND ABBREVIATIONS Version 1.1 28 May 2012 Distribution Statement	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINTY STAFF-MN/ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Objective 3.3 lexicon and abbreviations provides compilation of the existing definitions and terms from the various areas, legal terms and definitions associated to the cyber issues and relate strictly to the specific legal instrument, and custom made definitions or descriptions which are developed solely to the MNE 7 CD&E campaign.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**9**	

PREFACE

Objective 3.3 lexicon and abbreviations provides compilation of the existing definitions and terms from the various areas, legal terms and definitions associated to the cyber issues and relate strictly to the specific legal instrument, and custom made definitions or descriptions which are developed solely to the MNE 7 CD&E campaign.

Lexicon goal is to offer most suitable definitions or descriptions for the terms used, and create common understanding among participants as they consider the MNE 7 problem statement and baseline assessments, and engage in MNE 7 campaign activities and supporting endeavors. Lexicon will be a living document for the duration of the MNE 7 campaign.

Act of aggression means the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. Any of the following acts, regardless of a declaration of war, shall, in accordance with United Nations General Assembly resolution 3314 (XXIX) of 14 December 1974, qualify as an act of aggression:
(a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
(b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
(c) The blockade of the ports or coasts of a State by the armed forces of another State;
(d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
(e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
(f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
(g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein [Definition is for the purpose of paragraph 1 of the Rome Statute. Amendments to the Rome Statute of the International Criminal Court on the crime of aggression, Annex I, Article 8 *bis,* Crime of aggression, amendment is effective from June 11, 2010).

Attribution: Facts determining a method which caused the cyber incident and the entity that is responsible for it (MNE 7 Outcome 3 Working Definition).

Crime of aggression means the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations. [Definition is for the purpose of the Rome Statute. Amendments to the Rome Statute of the International Criminal Court on the crime of aggression, Annex I, Article 8 *bis,* Crime of aggression, amendment is effective from June 11, 2010).

Communication System: An assembly of equipment, methods and procedures and, if necessary, personnel, organized to accomplish information transfer functions. Notes: 1. A communication system provides communication between its users and may embrace transmission systems, switching systems and user systems. 2. A communication system may also include storage or processing functions in support of information transfer [AAP-6(2010), 29 May 2002].

Comprehensive Approach: The wide scope of actions in international crisis management, undertaken in a coordinated and collaborative manner with the affected nation(s). Co-ordination and collaboration includes national civilian government agencies and their defence and security forces, international and intergovernmental organisations, non-governmental organisations and the private sector to achieve greater harmonization in the analysis, planning, management, and evaluation of actions required to prevent, ameliorate, mitigate and/or resolve the conditions precipitating a crisis (USJFCOM: Conceptual Framework MNE 5; 2007).

Computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function (Convention on Cybercrime, Council of Europe. Entry in to force July 1, 2004).

Computer Network: A network of data processing nodes that are interconnected for the purpose of data communication [AAP-31(A)(2001), 11 Sept 1992].

Computer Network Attack: Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber attack [AAP-6(2010), 22 Jan 2002].

Computer Network Defence: Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks (Department of Defense Dictionary of Military and Associated Terms (Joint Publication 1-02), Department of Defense Dictionary of Military and Associated Terms, November 8, 2010).

Computer Network Operation: Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations (Department of Defense Dictionary of Military and Associated Terms (Joint Publication 1-02), Department of Defense Dictionary of Military and Associated Terms, November 8, 2010).

Computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data (Convention on Cybercrime, Council of Europe. Entry in to force July 1, 2004).

Critical Infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions (COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection).

Cyber Attack: A cyber attack is a cyber operation, whether offensive or defensive, which is reasonably expected to cause death or injury to persons or damage or destruction to objects [Manual on International Law Applicable to Cyber Warfare (MILCW). MILCW is a work in progress and final version of the manual is intended to be published in Fall 2012].

Cyber crime: An act which constitutes a crime under national and/or international criminal law, and which occurs in, or performed from, or uses cyber space (MNE 7 Outcome 3 Working Definition).

Cyber defence: The ability to prevent and mitigate effects of cyber attacks (MNE 7 Outcome 3 Working Definition).

Cyber disruption: Means any event with security relevance (MNE 7 Outcome 3 Working Definition).

Cyber espionage: Means illegal and covert activity of exploiting vulnerabilities and collecting protected information or intelligence in cyberspace (MNE 7 Outcome 3 Working Definition).

Cyber exploitation: Cyber exploitation refers to operations conducted through the use of computer networks in order to gather data from target information systems and networks. They are operations performed with the purpose of gathering technical or intelligence information, in order to enable and carry out other computer network operations. It can be labeled as intelligence activity, or as activity carried out with the purpose of preparing a cyber attack (MNE7 Outcome 3 working definition).

Cyberspace: Means all interconnected or autonomous physical and/or virtual networks, software-controlled systems and/or devices, software and data (MNE 7 Outcome 3 Working Definition).

Cyber incident: Any observable occurrence in a computer system or network which is violation or imminent threat of violation of security policies, or security procedures, or acceptable use policies, or constitutes a crime under national and/or international criminal law (MNE 7 Outcome 3 Working Definition).

Cyber security: The ability to protect, exploit and maintain control of the cyberspace (MNE 7 Outcome 3 Working Definition).

Cyber tactics: Execution of actions in order to achieve defined objectives (MNE 7 Outcome 3 Working Definition).

Cyberterrorism: Means adverse effects caused by the cyber attacks to intimidate or coerce society, or influence the policy of a government, or affect decision-making process of a government, or threaten national security (MNE 7 Outcome 3 Working Definition).

Cyber threat: Means the probability of a cyber attack that may result in unauthorized access to, manipulation of, exfiltration of, or impairment to the availability, integrity, confidentiality or nonrepudiation of an information system or information stored on or transiting an information system (MNE7 Outcome 3 working definition).

Cyber warfare: Any activity involving the use of data stream to achieve military objectives (MNE 7 Outcome 3 Working Definition).

Data: (1) A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. (2) Sometimes used as a synonym for documentation (IEEE Std. 610.12-1990).

Database: A collection of interrelated data stored together in one or more (IEEE Std. 610.12-1990).

Denial of Service (DoS): Prevention of authorized access to a system resources or the delaying of system operations and functions , with resultant loss of availability to authorized users (ISO/IEC 27033-1:2011).

Distributed Denial of Service (DDos): A Denial of Service technique that uses numerous hosts to perform the attack [National Information Assurance [IA] Glossary, Committee on National Security Systems, CNSS Instruction No. 4009,The Committee on National Security Systems (CNSS) Glossary Working Group (April 26, 2010)].

Domain: An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture [National Information Assurance [IA] Glossary, Committee on National Security Systems, CNSS Instruction No. 4009,The Committee on National Security Systems (CNSS) Glossary Working Group (April 26, 2010)].

Electromagnetic spectrum: The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands (Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02).

Freedom of Action: Within international standards and law, the liberty to conduct an activity at a given time and place without prohibitive and purposeful interference by others (Based on: MNE 7 Inter-Domain Baseline Assessment Report).

Global Commons: Areas that are potentially accessible to any and all actors – be they states, non-state, or individuals. Although this term is generally applied only to ungoverned access pathways between sovereign spaces or those areas that are outside the jurisdiction of any nation, MNE 7 will also address areas that fall under some degree of national sovereignty when they are relevant to ensuring access to and freedom of action within the global commons (Based on: MNE 7 Campaign Plan).

Hardware: Physical equipment used to process, store, or transmit computer programs or data (IEEE Standard Glossary of Software Engineering Terminology. The Institute of Electrical and Electronic Engineers (September 28, 1990).

Information: 1. The intelligence or knowledge capable of being represented in forms suitable for communication, storage or processing. *Notes:* 1. Information may be represented for example by signs, symbols, pictures or sounds. 2. In the context of the IEC definition "intelligence" should be taken in the broader meaning of the word. 3. Information may exist in the human mind, in document form and in electronic form. 2. (In information processing). The knowledge concerning objects, such as facts, events, things, processes or ideas including concepts, that within a certain context has a particular meaning. [AAP-31(A)(2001), 06 March 1992].

Information Assurance (IA): Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities [National Information Assurance [IA] Glossary, Committee on National Security Systems, CNSS Instruction No. 4009,The Committee on National Security Systems (CNSS) Glossary Working Group (April 26, 2010)].

Information Operations: The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (Joint Publications, SecDef Memo 12401-10).

Information system: means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance. (Council Framework Decision 2005/222/ JHA of 24 February 2005 on attacks against information systems).

Intelligence: The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity [AAP-6(2010), 01 Mar 1981].

Internet: The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN) [National Information Assurance [IA] Glossary, Committee on National Security Systems, CNSS Instruction No. 4009,The Committee on National Security Systems (CNSS) Glossary Working Group (April 26, 2010)].

Internet protocol (IP) address: Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks [National Information Assurance [IA] Glossary, Committee on National Security Systems,

CNSS Instruction No. 4009,The Committee on National Security Systems (CNSS) Glossary Working Group (April 26, 2010)].

Intranet: A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency) National Information Assurance [IA] Glossary, Committee on National Security Systems, CNSS Instruction No. 4009,The Committee on National Security Systems (CNSS) Glossary Working Group (April 26, 2010).

Limited Objective Experiment: A single, narrowly scoped, analytically focused event, employing one or more experimentation methods (either stand alone or part of an experimentation campaign) to focus on a single aspect of a larger problem (USA: Chairman of the Joint Chiefs of Staff Manual – CJCSM 3010.02. "Manual for Joint Concept Development and Experimentation"; 2010).

Malware: Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability. Note: viruses and Trojan horses are examples of malware (ISO/IEC 27033-1:2011).

Man-in-the-middle attack: A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association (National Information Assurance [IA] Glossary, Committee on National Security Systems, CNSS Instruction No. 4009,The Committee on National Security Systems (CNSS) Glossary Working Group (April 26, 2010).

Node: In communications and computer systems, the physical location that provides terminating, switching, and gateway access services to support information exchange (Department of Defense Dictionary of Military and Associated Terms, Joint Publication 6-0).

Risk: Probability and severity of loss linked to hazards (Department of Defense Dictionary of Military and Associated Terms, Joint Publication 5-0).

Service Provider means: (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service (Convention on Cybercrime, Council of Europe. Entry in to force July 1, 2004).

Software: Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system (IEEE Standard Glossary of Software Engineering Terminology. The Institute of Electrical and Electronic Engineers (September 28, 1990).

Structured Query Language (SQL) injection: Providing specially crafted parameters that will be combined within the Web service to generate a SQL query defined by the attacker (NIST SP800-95).

Vulnerability: 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment. 3. A weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system (Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02).

ABBREVIATIONS

AAP	(NATO) Allied Administrative Publication
ATC	Air Traffic Control
CCD COE	Cooperative Cyber Defence Centre of Excellence
CD&E	Concept Development and Experimentation
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructures
CIIP	Critical Information Infrastructure Protection
CMC	Computer Mediated Communication
CNA	Computer Network Attack
CND	Computer Network Defence
CNO	Computer Network Operations
DO-HQ	Deployable Operational Headquarter
EFMS	European Forum for Member States
EFTA	European Free Trade Association
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
ESS	European Security Strategy
EU	European Union
FOC	Full Operational Capability
FRS	Flight Reservation System
GA	General Assembly
GAL	Global Address List
GDMs	Guidelines for Decision Makers
ICC	International Criminal Court
ICJ	International Court of Justice
ICT	Information and Communication Technologies
ILC	International Law Commission
IOC	Initial Operational Capability
IP	Internet Protocol
ISP	Internet service Provider
ITU	International Telecommunication Union
JP	(USA) Joint Publication
LOE	Limited Objective Experiment
MS	Member States (EU)

MNE	Multinational Experiment
NATO	North Atlantic Treaty organization
NIS	Network and Information Security
OPSEC	Operational Security
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open Source Intelligence
PDA	Personal Digital Assistant
SME	Subject Matter Expert
SWGCA	Special Working Group on the Crime of Aggression
SQL	Structured Query Language
UNITAR	United Nations Institute of Training and Research
UNSCR	United Nations Security Council Resolution
VFR	Visual Flight Rules